

# Construction of a 3-dimensional MDS-code

DEDICATED TO THE CENTENARY OF THE BIRTH OF  
FERENC KÁRTESZI (1907-1989)

A. Aguglia and L. Giuzzi\*

## Abstract

In this paper, we describe a procedure for constructing  $q$ -ary  $[N, 3, N-2]$ -MDS codes, of length  $N \leq q+1$  (for  $q$  odd) or  $N \leq q+2$  (for  $q$  even), using a set of non-degenerate Hermitian forms in  $PG(2, q^2)$ .

## 1 Introduction

The well-known Singleton bound states that the cardinality  $M$  of a code of length  $N$  with minimum distance  $d$  over a  $q$ -ary alphabet always satisfies

$$M \leq q^{N-d+1}, \quad (1)$$

see [7]. Codes attaining the bound are called *maximum distance separable codes*, or *MDS* codes for short.

Interesting families of maximum distance separable codes arise from geometric and combinatorial objects embedded in a finite projective spaces. In particular linear  $[N, k, N-k+1]$ -MDS codes, with  $k \geq 3$ , and  $N$ -arcs in  $PG(k-1, q)$  are equivalent objects; see [1].

A general method for constructing a  $q$ -ary code is to take  $N$  multivariate polynomials  $f_1, \dots, f_N$  defined over a suitable subset  $\mathcal{W} \subseteq \text{GF}(q)^n$  and consider the set  $\mathcal{C}$  given by

$$\mathcal{C} = \{(f_1(x), \dots, f_N(x)) | x \in \mathcal{W}\}.$$

In this paper, we deal with the case  $|\mathcal{W}| = q^t$  and also assume that the *evaluation function*

$$\Theta : \begin{cases} \mathcal{W} \mapsto \mathcal{C} \\ x \mapsto (f_1(x), f_2(x), \dots, f_N(x)) \end{cases}$$

is injective.

---

\*Research supported by the Italian Ministry MIUR, Strutture geometriche, combinatoria e loro applicazioni.

If  $\mathcal{C}$  attains the Singleton bound then the restrictions of all the codewords to any given  $t = N - d + 1$  places must all be different, namely in any  $t$  positions all possible vectors occur exactly once. This means that a necessary condition for  $\mathcal{C}$  to be MDS is that any  $t$  of the varieties  $V(f_m)$  for  $m = 1, \dots, N$  meet in exactly one point in  $\mathcal{W}$ . Here  $V(f)$  denotes the algebraic variety associated to  $f$ .

Applying the above procedure to a set of non-degenerate Hermitian forms in  $PG(2, q^2)$  we construct some  $q$ -ary  $[N, 3, N-2]$ -MDS codes, of length  $N \leq q+1$  (for  $q$  odd) or  $N \leq q+2$  (for  $q$  even). The codes thus obtained can also be represented by sets of points in  $PG(3, q)$ ; this representation is used in Section 4 in order to devise an algebraic decoding procedure, based upon polynomial factorisation; see [9].

## 2 Preliminaries

Let  $\mathcal{A}$  be a set containing  $q$  elements. For any integer  $N \geq 1$ , the function  $d_H : \mathcal{A}^N \times \mathcal{A}^N \mapsto \mathbb{N}$  given by

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|,$$

is a metric on  $\mathcal{A}^N$ . This function is called the *Hamming distance* on  $\mathcal{A}^N$ . A  $q$ -ary  $(N, M, d)$ -code  $\mathcal{C}$  over the alphabet  $\mathcal{A}$  is just a collection of  $M$  elements of  $\mathcal{A}^N$  such that any two of them are either the same or at Hamming distance at least  $d$ ; see [4, 5]. The elements of  $\mathcal{C}$  are called *codewords* whereas the integers  $d$  and  $N$  are respectively the *minimum distance* and the *length* of  $\mathcal{C}$ .

If  $\mathcal{A} = GF(q)$  and  $\mathcal{C}$  is a  $k$ -dimensional vector subspace of  $GF(q)^N$ , then  $\mathcal{C}$  is said to be a *linear*  $[N, k, d]$ -code. Under several communication models, it is assumed that a received word  $\mathbf{r}$  should be decoded as the codeword  $\mathbf{c} \in \mathcal{C}$  which is nearest to  $\mathbf{r}$  according to the Hamming distance; this is the so-called maximum likelihood decoding. Under these assumptions the following theorem, see [4, 5], provides a basic bound on the guaranteed error correction capability of a code.

**Theorem 1.** *If  $\mathcal{C}$  is a code of minimum distance  $d$ , then  $\mathcal{C}$  can always either detect up to  $d - 1$  errors or correct  $e = \lfloor (d - 1)/2 \rfloor$  errors.*

Observe that the theorem does not state that it is not possible to decode a word more than  $e$  errors happened, but just that in this case it is possible that the correction fails. Managing to recover from more than  $e$  errors for some given received codewords is called “correcting beyond the bound”.

The *weight* of an element  $\mathbf{x} \in GF(q)^N$  is the number of non-zero components  $x_i$  of  $\mathbf{x}$ . For a linear code the minimum distance  $d$  equals the minimum weight of the non-zero codewords.

The parameters of a code are not independent; in general it is difficult to determine the maximum number of words a code of prescribed length  $N$  and minimum distance  $d$  may contain.

Observe that, for any arbitrary linear  $[N, k, d]$ -code, condition (1) may be rewritten as

$$d \leq N - k + 1; \quad (2)$$

thus  $\mathcal{C}$  is a linear MDS code if and only if equality holds in (2).

In Section 3 we shall make extensive use of some non-degenerate Hermitian forms in  $PG(2, q^2)$ .

Consider the projective space  $PG(d, q^2)$  and let  $V$  be the underlying vector space of dimension  $d + 1$ . A *sesquilinear Hermitian form* is a map

$$h : V \times V \longrightarrow GF(q^2)$$

additive in both components and satisfying

$$h(k\mathbf{v}, l\mathbf{w}) = kl^qh(\mathbf{v}, \mathbf{w})$$

for all  $\mathbf{v}, \mathbf{w} \in V$  and  $k, l \in GF(q^2)$ . The form is *degenerate* if and only if the subspace  $\{\mathbf{v} \mid h(\mathbf{v}, \mathbf{w}) = 0 \ \forall \mathbf{w} \in V\}$ , the *radical* of  $h$ , is different from  $\{\mathbf{0}\}$ . Given a sesquilinear Hermitian form  $h$ , the associated Hermitian variety  $\mathcal{H}$  is the set of all points of  $PG(d, q^2)$  such that  $\{< \mathbf{v} > \mid \mathbf{0} \neq \mathbf{v} \in V, h(\mathbf{v}, \mathbf{v}) = 0\}$ . The variety  $\mathcal{H}$  is *degenerate* if  $h$  is degenerate; non-degenerate otherwise. If  $h$  is a sesquilinear Hermitian form in  $PG(d, q^2)$  then the map  $F : V \longrightarrow GF(q)$  defined by

$$F(\mathbf{v}) = h(\mathbf{v}, \mathbf{v}),$$

is called *the Hermitian form on  $V$  associated to  $h$* . The Hermitian form  $F$  is *non-degenerate* if and only if  $h$  is non-degenerate. Complete introductions to Hermitian forms over finite fields may be found in [2, 6].

### 3 Construction

Let  $S$  be a transversal in  $GF(q^2)$  of the additive subgroup  $T_0 = \{y \in GF(q^2) : T(y) = 0\}$ , where  $T : y \in GF(q^2) \mapsto y^q + y \in GF(q)$  is the trace function. Denote by  $\Lambda$  the subset of  $GF(q^2)$  satisfying

$$\left(\frac{\alpha - \beta}{\gamma - \beta}\right)^{q-1} \neq 1 \quad (3)$$

for any  $\alpha, \beta, \gamma \in \Lambda$ . Choose a basis  $B = \{1, \varepsilon\}$  of  $GF(q^2)$ , regarded as a 2-dimensional vector space over  $GF(q)$ ; hence, it is possible to write each element  $\alpha \in GF(q^2)$  in components  $\alpha_1, \alpha_2 \in GF(q)$  with respect to  $B$ . We may thus identify the elements of  $GF(q^2)$  with the points of  $AG(2, q)$ , by the bijection

$$(x, y) \in AG(2, q) \mapsto x + \varepsilon y \in GF(q^2).$$

Condition (3) corresponds to require that  $\Lambda$ , regarded as point-set in  $AG(2, q)$ , is an arc. Thus, setting  $N = |\Lambda|$ , we have

$$N \leq \begin{cases} q + 1 & \text{for } q \text{ odd} \\ q + 2 & \text{for } q \text{ even.} \end{cases} \quad (4)$$

Now, consider the non-degenerate Hermitian forms  $\mathcal{F}_\lambda(X, Y, Z)$  on  $GF(q^2)^3$

$$\mathcal{F}_\lambda(X, Y, Z) = X^{q+1} + Y^q Z + Y Z^q + \lambda^q X^q Z + \lambda X Z^q,$$

as  $\lambda$  varies in  $\Lambda$ . Label the elements of  $\Lambda$  as  $\lambda_1, \dots, \lambda_N$  and let  $\Omega = GF(q^2) \times S$ .

**Theorem 2.** *The set*

$$\mathcal{C} = \{(\mathcal{F}_{\lambda_1}(x, y, 1), \mathcal{F}_{\lambda_2}(x, y, 1), \dots, \mathcal{F}_{\lambda_N}(x, y, 1)) | (x, y) \in \Omega\}$$

*is a  $q$ -ary linear  $[N, 3, N-2]$ -MDS code.*

*Proof.* We first show that  $\mathcal{C}$  consists of  $q^3$  tuples from  $GF(q)$ . Let  $(x_0, y_0), (x_1, y_1) \in \Omega$  and suppose that for any  $\lambda \in \Lambda$ ,

$$\mathcal{F}_\lambda(x_0, y_0, 1) = \mathcal{F}_\lambda(x_1, y_1, 1).$$

Then,

$$T(\lambda(x_1 - x_0)) = x_0^{q+1} - x_1^{q+1} + T(y_0 - y_1). \quad (5)$$

In particular,

$$T(\lambda(x_1 - x_0)) = T(\alpha(x_1 - x_0)) = T(\gamma(x_1 - x_0)) \quad (6)$$

for any  $\alpha, \lambda, \gamma \in \Lambda$ .

If it were  $x_1 \neq x_0$ , then (6) would imply

$$\left(\frac{\alpha - \beta}{\gamma - \beta}\right)^{q-1} = 1,$$

contradicting the assumption made on  $\Lambda$ . Therefore,  $x_1 = x_0$  and from (5) we get  $T(y_0 - y_1) = 0$ . Hence,  $y_0$  and  $y_1$  are in the same coset of  $T_0$ ; by definition of  $S$ , it follows that  $y_0 = y_1$ , thus  $\mathcal{C}$  has as many tuples as  $|\Omega|$ .

We are now going to show that  $\mathcal{C}$  is a vector subspace of  $GF(q)^N$ . Take  $(x_0, y_0), (x_1, y_1) \in \Omega$ . For any  $\lambda \in \Lambda$ ,

$$\mathcal{F}_\lambda(x_0, y_0, 1) + \mathcal{F}_\lambda(x_1, y_1, 1) = \mathcal{F}_\lambda(x_2, y_2, 1), \quad (7)$$

where  $x_2 = x_0 + x_1$  and  $y_2 = y_0 + y_1 - x_0^q x_1 - x_1^q x_0$ . Likewise, for any  $\kappa \in GF(q)$ ,

$$\kappa \mathcal{F}_\lambda(x_0, y_0, 1) = \mathcal{F}_\lambda(x, y, 1), \quad (8)$$

where  $x = \kappa x_0$  and  $y$  is a root of

$$y^2 + y = (\kappa - \kappa^2)x_0^{q+1} + \kappa(y_0^q + y_0).$$

Therefore,  $\mathcal{C}$  is a vector subspace of  $GF(q)^N$ ; as it consists of  $q^3$  tuples,  $\mathcal{C}$  is indeed a 3-dimensional vector space.

Finally we prove that the minimum distance  $d$  of  $\mathcal{C}$  is  $N-2$ . Since  $\mathcal{C}$  is a vector subspace of  $GF(q)^N$ , its minimum distance is  $N-z$ , where

$$z = \max_{\substack{\mathbf{c} \in \mathcal{C} \\ \mathbf{c} \neq \mathbf{0}}} |\{i : c_i = 0\}|.$$

First observe that  $z \geq 2$  because of Singleton bound (2). In order to show that  $z = 2$  we study the following system

$$\begin{cases} \mathcal{F}_\alpha(x, y, 1) = 0 \\ \mathcal{F}_\beta(x, y, 1) = 0 \\ \mathcal{F}_\gamma(x, y, 1) = 0 \end{cases} \quad (9)$$

for  $\alpha, \beta, \gamma$  distinct elements of  $\Lambda$ . Set  $U = x^{q+1} + y^q + y$ ,  $V = x^q$  and  $W = x$ ; then, (9) becomes

$$\begin{cases} U + \alpha^q V + \alpha W = 0 \\ U + \beta^q V + \beta W = 0 \\ U + \gamma^q V + \gamma W = 0 \end{cases} \quad (10)$$

Since  $\left(\frac{\alpha-\beta}{\gamma-\beta}\right) \neq 1$ , the only solution of (10) is  $U = V = W = 0$ , that is  $x = 0$  and  $y + y^q = 0$ . In particular, there is just one solution to (9) in  $\Omega$ , that is  $\mathbf{x} = (0, 0)$ . This implies that a codeword which has at least three zero components is the zero vector, hence  $z = 2$  and thus the minimum distance of  $\mathcal{C}$  is  $N - 2$ .  $\square$

**Example.** When  $q$  is odd, a transversal  $S$  for  $T_0$  is always given by the subfield  $\text{GF}(q)$  embedded in  $\text{GF}(q^2)$ . In this case it is then extremely simple to construct the code. For  $q = 5$ , a computation using GAP [3], shows that in order for  $\Lambda$  to satisfy property (3), we may take  $\Lambda = \{\varepsilon^3, \varepsilon^4, \varepsilon^8, \varepsilon^{15}, \varepsilon^{16}, \varepsilon^{20}\}$ , where  $\varepsilon$  is a root of the polynomial  $X^2 - X + 2$ , irreducible over  $\text{GF}(5)$ . The corresponding Hermitian forms are

$$\begin{aligned} X^{q+1} + Y^q Z + y Z^q + \varepsilon^{15} X^q Z + \varepsilon^3 X Z^q \\ X^{q+1} + Y^q Z + Y Z^q + \varepsilon^{20} X^q Z + \varepsilon^4 X Z^q \\ X^{q+1} + Y^q Z + Y Z^q + \varepsilon^{16} X^q Z + \varepsilon^8 X Z^q \\ X^{q+1} + Y^q Z + Y Z^q + \varepsilon^3 X^q Z + \varepsilon^{15} X Z^q \\ X^{q+1} + Y^q Z + Y Z^q + \varepsilon^8 X^q Z + \varepsilon^{16} X Z^q \\ X^{q+1} + Y^q Z + Y Z^q + \varepsilon^4 X^q Z + \varepsilon^{20} X Z^q \end{aligned}$$

A generator matrix for the  $[6, 3, 4]$ -MDS code obtained applying Theorem 2 to these Hermitian forms is,

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 2 & 1 & 2 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix}$$

*Remark 1.* In  $PG(2, q^2)$ , take the line  $\ell_\infty : Z = 0$  as the line at infinity. Then, in the affine space  $AG(2, q^2) = PG(2, q^2) \setminus \ell_\infty$ , any two Hermitian curves  $V(F_\lambda)$  have  $q^2$  affine points in common,  $q$  of which in  $\Omega \subset AG(2, q^2)$ . Likewise, the full intersection

$$\bigcap_{\lambda \in \Lambda} V(F_\lambda)$$

consists of the  $q$  affine points  $\{(0, y) | y^q + y = 0\}$ , corresponding to just a single point in  $\Omega$ .

*Remark 2.* Denote by  $A_i$  the number of words in  $\mathcal{C}$  of weight  $i$ . Since  $\mathcal{C}$  is an MDS code, we have

$$A_i = \binom{N}{i} (q-1) \sum_{j=0}^{i-N+2} (-1)^j \binom{i-1}{j} q^{i-j-N+2};$$

see [8]. Thus,

$$\begin{aligned} A_{N-2} &= \frac{1}{2}(N^2 - N)(q-1) \\ A_{N-1} &= Nq^2 - (N^2 - N)q + N^2 - 2N \\ A_N &= q^3 - Nq^2 + \frac{1}{2}((N^2 - N)q - N^2 + 3N). \end{aligned}$$

## 4 Decoding

In this section it will be shown how the code  $\mathcal{C}$  we constructed may be decoded by geometric means.

Our approach is based upon two remarks:

1. Any received word  $\mathbf{r} = (r_1, \dots, r_N)$  can be uniquely represented by a set  $\tilde{\mathbf{r}}$  of  $N$  points of  $PG(3, q)$

$$\tilde{\mathbf{r}} = \{(\lambda_i^1, \lambda_i^2, r_i, 1) : \lambda = \lambda_i^1 + \varepsilon \lambda_i^2 \in \Lambda\}.$$

These points all lie on the cone  $\Psi$  of basis

$$\Xi = \{(\lambda_i^1, \lambda_i^2, 0, 1) : \lambda = \lambda_i^1 + \varepsilon \lambda_i^2 \in \Lambda\}$$

and vertex  $Z_\infty = (0, 0, 1, 0)$ .

2. The function

$$\phi_{(a,b)}(x, y, z, t) = (a^{q+1} + T(b))t + T((x + \varepsilon y)a)$$

is a homogeneous linear form defined over  $GF(q)^4$  for any  $a, b \in GF(q^2)$ .

Recall that the codeword  $\mathbf{c}$  corresponding to a given  $(a, b) \in \Omega$  is

$$\mathbf{c} = (\phi_{(a,b)}(\lambda_1^1, \lambda_1^2, 0, 1), \phi_{(a,b)}(\lambda_2^1, \lambda_2^2, 0, 1), \dots, \phi_{(a,b)}(\lambda_N^1, \lambda_N^2, 0, 1));$$

thus,  $\tilde{\mathbf{c}}$ , the set containing the points  $(\lambda_i^1, \lambda_i^2, c_i, 1)$ , is the full intersection of the plane  $\pi_{a,b} : z = \phi_{(a,b)}(x, y, z, t)$  with the cone  $\Psi$ .

It is clear that knowledge of the plane  $\pi_{(a,b)}$  is enough to reconstruct the codeword  $\mathbf{c}$ . In the presence of errors, we are looking for the nearest codeword  $\mathbf{c}$  to a vector  $\mathbf{r}$ ; this is the same as to determine the plane  $\pi_{(a,b)}$  containing most of the points of  $\tilde{\mathbf{r}}$ . In order to obtain such a plane, we adopt the following approach. Assume  $\ell$  to be a line of the plane  $\pi_{0,0} : z = 0$  external to  $\Xi$  and denote by  $\pi_\infty$  the plane at infinity of equation  $t = 0$ . For any  $P \in \ell$ , let  $\tilde{\mathbf{r}}^P$  be the projection from  $P$  of the set  $\tilde{\mathbf{r}}$  on  $\pi_\infty$ . Write  $\mathcal{L}_{\mathbf{r}}^P$  for a curve of  $\pi_\infty$  of minimum degree containing  $\tilde{\mathbf{r}}^P$ . Observe that  $\deg \mathcal{L}_{\mathbf{r}}^P \leq q + 1$  and  $\deg \mathcal{L}_{\mathbf{r}}^P = 1$  if, and only if, all the points of  $\tilde{\mathbf{r}}$  lie on a same plane through  $P$ , that is  $\tilde{\mathbf{r}}$  corresponds to a codeword associated with that plane passing through  $P$ .

We now can apply the following algorithm using, for example, [3].

1. Take  $P \in \ell$ ;
2. Determine the projection  $\mathbf{r}^P$  and compute the curve  $\mathcal{L}_{\mathbf{r}}^P$ ;
3. Factor  $\mathcal{L}_{\mathbf{r}}^P$  into irreducible factors, say  $\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_v$ ;
4. Count the number of points in  $\tilde{\mathbf{r}}^P \cap V(\mathcal{L}_i)$  for any factor  $\mathcal{L}_i$  of  $\mathcal{L}_{\mathbf{r}}^P$  with  $\deg \mathcal{L}_i = 1$ .
5. If for some  $i$  we have  $n_i > \frac{N+1}{2}$ , then return the plane spawned by  $P$  and two points of  $\mathcal{L}_i$ ; else, as long as not all the points of  $\ell$  have been considered, return to point 1.
6. If no curve with the required property has been found, return failure.

*Remark 3.* The condition on  $n_i$  in point 5 checks if the plane contains more than half of the points corresponding to the received word  $\mathbf{r}$ ; when this is the case, a putative codeword  $\mathbf{c}$  is constructed, with  $d(\mathbf{c}, \mathbf{r}) \leq \frac{N-3}{2}$ ; thus, when  $\mathbf{c} \in \mathcal{C}$ , then it is indeed the unique word of  $\mathcal{C}$  at minimum distance from  $\mathbf{r}$ . However, the aforementioned algorithm may be altered in several ways, in order to be able to try to correct errors beyond the bound; possible approaches are

1. iterate the procedure for all the points on  $\ell$  and return the planes containing most of the points corresponding to the received vector;
2. use some further properties of the cone  $\Psi$ ; in particular, when  $\Xi$  is a conic it seems possible to improve the decoding by considering also the quadratic components of the curve  $\mathcal{L}_{\mathbf{r}}^P$ .

*Remark 4.* The choice of  $P$  on a line  $\ell$  is due to the fact that any line of  $\pi_{0,0}$  meets all the planes of  $\text{PG}(3, q)$ . In general, we might have chosen  $\ell$  to be just a blocking set disjoint from  $\Xi$ . Observe that when  $q$  is odd and  $|\Lambda| = q + 1$ , then the line  $\ell$  is just an external line to a conic of  $\pi_{0,0}$ .

## References

- [1] E.F. Assmus Jr and J.D. Key. *Designs and their codes*, Cambridge University Press (1992).
- [2] S.N. Bose and I.M. Chakravarti, *Hermitian varieties in a finite projective space*  $\text{PG}(N, q^2)$ , *Canad J. Math.* **18** (1966), 1161–1182.
- [3] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4* (2006) (`\protect\vrule width0pt\protect\href{http://www.gap-system.org}{http://www.gap-system.org}`)
- [4] L. Giuzzi, *Codici correttori*, Springer–Verlag (2006).
- [5] R. McEliece, *Theory of Information and coding*, Cambridge University Press (2002).
- [6] B. Segre, *Forme e geometrie hermitiane, con particolare riguardo al caso finito*, *Ann. Mat. Pura Appl. (4)* **70** (1965), 1–201.
- [7] R. C. Singleton, *Maximum distance  $q$ -nary codes*, *IEEE Trans. Inf. Theory* **10** issue 2 (1964), 116–118.
- [8] L. Staiger, *On the weight distribution of linear codes having dual distance  $d' > k$* , *IEEE Trans. Inf. Theory* **35** issue 1 (1989), 186–188.
- [9] M. Sudan, *Decoding Reed Solomon codes beyond the error-correction bound*, *Journal of Complexity*, **13** issue 1 (1997), 180–193

ANGELA AGUGLIA  
Dipartimento di Matematica  
Politecnico di Bari  
Via G. Amendola 126/B  
70126 Bari  
Italy  
a.aguglia@poliba.it

LUCA GIUZZI  
Dipartimento di Matematica  
Politecnico di Bari  
Via G. Amendola 126/B  
70126 Bari  
Italy  
l.giuZZi@poliba.it